From: Chen, Lily (Fed)
To: Moody, Dustin
Subject: RE: PQC NISTIR Comments
Date: Wednesday, March 9, 2016 8:33:00 AM

Dustin:

You can pick any one. Remember, we need on Division reader who should be in the division. Another is WERB reader, we can ask an external. A NSA guy will work.

Lily

From: Moody, Dustin (Fed)
Sent: Wednesday, March 09, 2016 8:18 AM
To: Chen, Lily (Fed)
Subject: Re: PQC NISTIR Comments

Anybody you had in mind? Or should I pick?

Also, do we want to just leave this as a NISTIR? or publish in the NIST Journal of Research or something similar?

Dustin

From: Chen, Lily (Fed)

Sent: Wednesday, March 9, 2016 8:13 AM

To: Moody, Dustin (Fed); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Perlner, Ray (Fed); Peralta, Rene (Fed)

Subject: RE: PQC NISTIR Comments

Hi, Dustin:

As we are revising IR 8105, I think we can identify readers for the WERB procedure to get them start to read now.

Lily

From: Moody, Dustin (Fed)
Sent: Wednesday, March 09, 2016 8:01 AM
To: Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Perlner, Ray (Fed); Peralta, Rene (Fed); Chen, Lily (Fed)
Subject: PQC NISTIR Comments

Everyone,

The comment period for our PQC NISTIR ends tomorrow. We've received only five comments back, with one more to come next week. I've included them below. I don't think we need to make any real changes in the NISTIR. Let me know if you have any other thoughts.

Dustin

Comments received on our PQC NISTIR 8105

Ludovic Perret

- I am writing you regard the document « Report on Post-Quantum Cryptography » which provides a reasonable view of the current state-of-the
  art of post-quantum cryptography. Of course, I am happy that NIST is taking a position to push the community forward on the transition.
  I have one question regarding the last part of the document :
  « While this process will have many commonalities with the processes that led to the standardization of AES [20] and SHA3 [21], this is not a competition. NIST sees its role as managing a process of achieving community consensus in a transparent and timely manner. Ideally, several algorithms will emerge as "good choices". NIST may pick one or more of these for standardization in each category. In this respect, NIST's process for standardizing quantum resistant public key cryptography will be similar to the ongoing block cipher modes

development process [22]. »
I am not sure, but is the « ongoing block cipher modes development process » is referring to the CAESAR competition http://competitions.cr.yp.to/index.html ?
So, are you expecting that academics somewhat organize the selection process ?

Hildegard Ferraiolo (NIST)

- Table 1 depicts the "Impact of Quantum Computing on Common Cryptographic Algorithms" showing impacts on signature, encryption, hashing functions, and key exchange. There is no impact on 'authentication'. Authentication, however, is the front door to many off the "functions outlined in table 1.

  Please consider authentication as one of the rows in table 1.

recommend that the statement (and especially the bolded statement):

It is critical to engage with the community for NIST cryptographic standards to be endorsed by industry and other standards organizations around the world. **This Internal Report shares NIST's current understanding about the status of quantum computing and post-quantum cryptography. The Report also outlines our initial plan to move forward.**

Recommendation:

NIST IR's goal (as highlighted in bold) should take more prominence and be introduced earlier in the document.

Michael Harris (CDC)

- Please expand on "crypto agility" and concrete things agencies/users can do to maintain it.
  - Possible examples:
    - (1) Migrate to stronger symmetric encryption and hashing now. Give detail on necessary configurations (e.g. key sizes, specific algorithms).
    - (2) Avoid getting locked in to any specific crypto implementations (include flexibility in policies, planning, processes, procedures, procurement, and technology) and become ready and able to rapidly swap things in and out.
    - (3) As early as 2023, it may be necessary to budget for some very significant retrofitting of entire security infrastructure if quantum computing has advanced enough that a rapid rather than gradual response is necessitated (could discuss scope of what needs to be considered for this planning).

David Hook (Crypto Workshop LLC)

would like to suggest something to consider during the transition phase while new algorithms for post-quantum cryptography are being chosen.

At the moment there is a reasonable body of research supporting the security of key exchange methods based around Ring-learning-with-errrors (Ring-LWE). If my understanding is correct an algorithm implementing Ring-LWE should be disabled (as should any other non-approved algorithm) if a module which supports a Ring-LWE algorithm, such as NewHope, is running in FIPS approved mode.

I would like to suggest as an interim measure that the restriction requiring the disablement of these algorithms be relaxed if they are only used for the purpose of calculating material to go in the SuppPrivInfo component of the OtherInfo data described in Section 5.8.1.2 of SP 800-56A Revision 2. This condition could be outlined in the guidance section of the module's security policy.

At the worst this will not weaken the regular key agreement algorithms, at best, assuming no new research shows up suggesting Ring-LWE techniques are somehow flawed, it will have the effect of "post-quantum hardening" the key agreement calculations, as in addition to the regular key agreement value, another input to the KDF will be the key exchange value calculated using the Ring-LWE algorithm.

I think allowing this relaxation will also stimulate a lot of use and investigation into these algorithms as well, in a variety of ways. They do seem to be very different beasts to what we are used to dealing with, and in this case, where the use of them should do no harm, it would be worth providing some encouragement to allow their use in "real world"
applications. Choosing candidates for quantum-resistant cryptography is one thing, having good ways of applying the candidates is quite another.
[1] https://cryptojedi.org/papers/newhope-20151207.pdf "Post-quantum key exchange – a new hope", Alkim, Ducas, et al.

David Jao (University of Waterloo)

My name is David Jao. I am the designer of post-quantum cryptosystems based on the isogeny problem over supersingular elliptic curves.

I was pleased to see that isogeny-based cryptosystems are included in the overview of post-quantum cryptosystems on page 4 of NIST IR 8105. On that page, you state regarding isogeny-based cryptosystems that "there has not been enough analysis to have much confidence in their security." While I certainly agree with this statement, I hope that you will disclose the eventual criteria that you use to determine whether or not a system has had enough analysis. In particular, you also state on page 5 of NIST IR 8105 that "more research and analysis are needed before any of the above proposed post-quantum cryptosystems could be recommended for use today." This second statement implies that all of the main families of post-quantum primitives in your overview suffer from a lack of analysis, raising the question of why exactly isogeny-based cryptosystems are any worse than the others in this aspect. I hope that, in the final decision, uniform and published criteria will be applied to the evaluation of the proposals. Of course, there may exist objective criteria (such as date of earliest publication) which would favor one family over another. I emphasize here only the need for transparency because past experience has shown that NIST is at its best when the selection process is open and publicly visible.

On page 4 of the report, you state: "One challenge that will likely need to be overcome is that most of the quantum resistant algorithms have larger key sizes than the algorithms they will replace." I think it is important to emphasize just how important the key size constraint really is, and I would like to see key size considerations represented adequately in your eventual evaluation criteria. Many of the authors of NIST IR 8105 attended Dan Bernstein's talk at PQCrypto 2016 in which he discussed the network packet size (MTU) limits that are hard-coded into today's internet protocols. Most extant IPv4 hardware can only handle single network packets of a maximum size of 1500 bytes. For IPv6, the practical limit is 1280 maximum bytes in a single packet. Changing these limits is nearly impossible since it would require wholesale replacement of all existing internet hardware as well as making an incompatible change to fundamental internet protocols. Cryptography software in a malicious environment often must operate under the assumption that a public key must fit entirely in a single network packet, because multiple packets are too easy for an attacker to manipulate. Current protocols such as TLS and Tor are built with this assumption in mind. After accounting for protocol overhead, there are very few post-quantum primitives available today that can fit an entire public key into a single network packet at the 128-bit security level, and almost none that can do so at the 256-bit security level. You may find it

interesting that recent work of myself and others (https://eprint.iacr.org/2016/229), to appear in AsiaPKC 2016, shows that isogeny public keys can fit into 384 bytes at the 128-bit security level and 768 bytes at the 256-bit security level. These numbers outperform every other post-quantum cryptographic primitive in the literature, even though our key size estimates are based entirely on quantum cryptanalysis whereas several of our closest competitors in this metric (such as QC-MDPC codes) admit to date only published estimates based on classical cryptanalysis.

The entire research community as well as the business sector is grateful to NIST for providing this forum to showcase the latest progress in post-quantum cryptography. It is wonderful to see NIST being proactive instead of reactive on this extremely critical issue.

Mike Stewart (US Navy)

- He will send us a comment next week.